(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/30018 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/EP00/09866

(22) International Filing Date: 4 October 2000 (04.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99203414.0 18 October 1999 (18.10.1999) EP

(71) Applicant *(for all designated States except US)*: **IRDETO ACCESS B.V.** [NL/NL]; Jupiterstraat 42, NL-2132 HD Hoofddorp (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WAJS, Andrew, Augustine** [GB/NL]; Schotersingel 93, NL-2023 AA Haarlem (NL).

(74) Agent: **DE VRIES, Johannes, Hendrik, F.**; De Vries & Metman B.V., Overschiestraat 180, NL-1062 XK Amsterdam (NL).

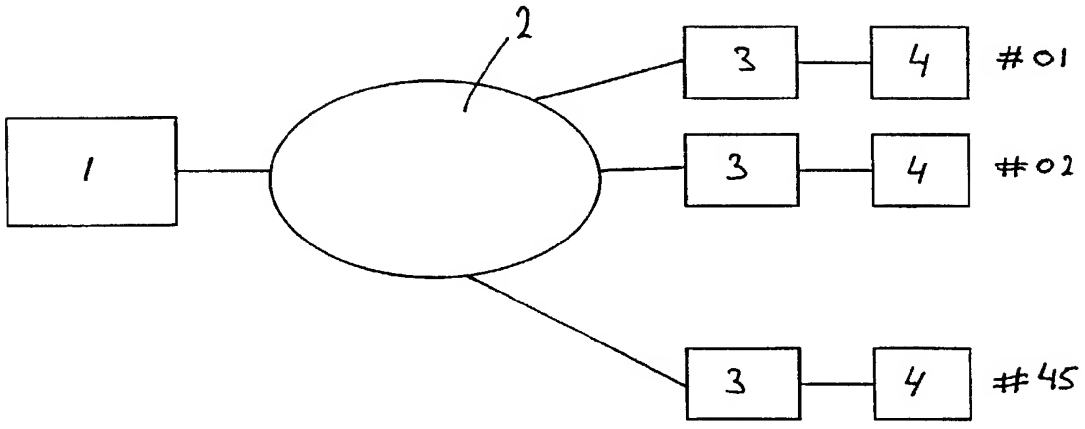
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR DISTRIBUTING KEYS AMONG A NUMBER OF SECURE DEVICES, METHOD FOR COMMUNICATING WITH A NUMBER OF SECURE DEVICES, SECURITY SYSTEM, AND SET OF SECURE DEVICES



(57) Abstract: In a method for distributing keys among a number of secure devices, the secure devices are divided into sets (A, B, C, D, E), each set having a plurality of subsets (a, b, c, d, e). Each subset comprises two or more secure devices having the same key which is unique for this subset. Each secure device is a member of a number of sets (A, B, C, D, E) such that two or more secure devices which are a member of a subset, are not a member of the same subset in another set.

WO 01/30018 A1

Method for distributing keys among a number of secure devices, method for communicating with a number of secure devices, security system, and set of secure devices

The invention relates to a method for distributing keys among a number of secure devices. The invention further relates to a method for communicating with a number of secure devices, to a security system in which this method is used, and to a set of secure devices obtained by the distributing method.

It is known to protect content against unauthorised copying by using conditional access like technology. The term content in the present application is used as an indication of any type of information, such as audio or video signals, computer software etc. To protect the content, the content is scrambled using a control word. The term "control word" refers to the key which is used in the scrambling algorithm to scramble the content. The control word is generally transferred to the descrambling location in an encrypted message. In a consumer electronic system, such as for example a CD or DVD player or a PC, a secure device, such as a smart card, is used to decrypt the encrypted message to obtain the control word and the decrypted control word is used by the electronic system to descramble the content. As a large number of secure devices is open to attack by hackers, it is not unlikely on the long term that the security of a secure device will be breached so that the content is available for unauthorized commercial purposes. In a commonly used method in conditional access systems, breaches of security are managed by distributing new keys which are used to encrypt the control word. However in particular in off-line circumstances, i.e. in case of distribution of scrambled content on CD's and DVD's, for example, such a distribution method can not be used.

The invention aims to provide a method for distributing keys among a number of secure devices, which is in particular suitable for distributing keys in stored media applications.

It is a further object of the invention to provide a method for communicating with a number of secure devices.

The invention further aims to provide a method for scrambling a content and a method for descrambling a scrambled content, in particular for use with stored media applications.

Moreover, it is an object of the invention to provide a security system, in which these methods are used.

Finally the invention aims to provide a set of secure devices obtained by the method for distributing keys.

According to the invention a method for distributing keys among a number of secure devices is provided, wherein the secure devices are divided into sets, each set having a plurality of subsets, each subset comprising two or more secure devices having the same key which is unique for this subset, wherein each secure device is a member of a number of sets such that two or more secure devices which are a member of a subset, are not a member of the same subset in another set.

In this manner a method is obtained, wherein the secure devices will be provided with a number of keys, so that in case security of one secure device is breached, the keys stored in this secure device can be cancelled for future use so that this breached secure device is useless, while the other secure devices can use the remaining keys available to these secure devices.

According to the invention the method for communicating with a number of secure devices, comprising providing a number of unique keys, said number of keys being divided into subsets (A,a;A,b;...E,d;E,e), providing a plurality of encrypted messages by encrypting at least one clear message using different keys of said number of keys, adding an identifier to each encrypted message identifying the key used, wherein only a plurality of the available number of keys are

used to provide said encrypted messages, forwarding the encrypted messages to the secure devices, and decrypting the encrypted message in the secure device to obtain the clear message.

For scrambling a content for distribution among a number of users, the method of the invention comprises scrambling the content using a control word, wherein the control word is said clear message, wherein the scrambled content and the number of encrypted control messages are forwarded to all users.

The method for descrambling a scrambled content of the invention, comprises receiving the scrambled content and receiving a plurality of encrypted control messages, each encrypted control message having an identifier and containing a control word encrypted using a different key identified by the corresponding identifier, retrieving a first key identifier from a secure device having a plurality of keys with key identifiers, searching for an encrypted control message having an identifier corresponding to the retrieved identifier and decrypting in the secure device the encrypted control message found to obtain the control word, and descrambling the scrambled content by using the control word.

A security system of the invention comprises a plurality of terminals and a plurality of secure devices, each secure device comprising a processor and a memory for storing keys, wherein the secure devices are divided into sets (A,B,C,D,E), each set having a plurality of subsets (a,b,c,d,e), each subset being assigned a unique key from a number of unique keys (A,a;A,b;...E,d;E,e) and each subset comprising two or more of the secure devices, wherein the memory of each secure device contains a plurality of keys unique to different subsets such that the memory of each secure device contains a unique combination of unique subset keys, each terminal comprising means for forwarding an encrypted message to a secure device communicating with the terminal, wherein each encrypted message is obtained by encrypting at least one clear message using different keys of said number of keys, adding an identifier to each encrypted

message identifying the key used, wherein only a plurality of the available number of keys are used to provide said encrypted messages, and decrypting the encrypted message in the secure device to obtain the clear message for further use.

Finally, the invention provides a set of secure devices, such as smart cards, each secure device comprising a processor and a memory for storing keys, wherein the secure devices are divided into sets, each set having a plurality of subsets, each subset being assigned a unique key and each subset comprising two or more of the secure devices, wherein the memory of each secure device contains a plurality of keys unique to different subsets such that the memory of each secure device contains a unique combination of unique subset keys.

The invention will be further explained by reference to the drawing.

Fig. 1 schematically shows a content provider and a number of users of the content.

Fig. 2 shows a system for descrambling a scrambled content with a secure device.

Fig. 1 shows a content provider system 1 operating according to an embodiment of the method for scrambling a content according to the invention. The scrambled content is distributed among a number of users by means of a distribution network 2. This distribution network 2 can be, for example, the Internet, a broadcast network or a number of shops selling CD's, DVD's or other storage media. Each user has a system 3 for descrambling the scrambled content cooperating with a secure device 4, such as a smart card. The system 3 can be part of a CD or DVD player, a PC or can be implemented by means of a suitable software program running on a microprocessor which is part of such equipment.

In order to prevent unauthorized copying of the content provided by the system 1, a provider will scramble the content using a suitable scrambling algorithm, wherein a key is used to scramble this content. The key used to scramble the content will be indicated as control word in this

description. The control word is delivered to the users as an encrypted control message or cryptogram. It is noted that this control message may contain further entitlement information such as number of uses of the content, period during which the content may be used or the like. This part of the control message is not part of the present invention and will not be described further. The control message is encrypted using a key which is unique to the secure device 4 of a restricted number of users only. The manner in which the keys are distributed among a number of secure devices 4 will explained by reference to the following example.

A				
a	b	c	d	e
01	11	21	31	41
02	12	22	32	42
03	13	23	33	43
04	14	24	34	44
05	15	25	35	45

B				
a	b	c	d	e
01	11	21	31	41
42	02	12	22	32
33	43	03	13	23
24	34	44	04	14
15	25	35	45	05

C				
a	b	c	d	e
01	11	21	31	41
32	42	02	12	22
13	23	33	43	03
44	04	14	24	34
25	35	45	05	15

D				
a	b	c	d	e
01	11	21	31	41
22	32	42	02	12
43	03	13	23	33
14	24	34	44	04
35	45	05	15	25

E				
a	b	c	d	e
01	11	21	31	41
12	22	32	42	02
23	33	43	03	13
34	44	04	14	24
45	05	15	25	35

As indicated in these tables, the secure devices are divided into sets A,B,C,D and E and each set has a plurality of subsets a,b,c,d and e. Subset A,a comprises secure devices #01-#05, subset A,b comprises secure devices #11-#15, subset A,c comprises secure devices #21-#25, subset A,d comprises secure devices #31-#35 and subset A,e comprises secure devices #41-#45. The secure devices of each subset receive the same unique key, for example the secure devices #01-#05 of subset A,a receive the unique key A,a. This means that for example secure device #01 has the following set of unique keys A,a; B,a; C,a; D,a and E,a. As shown in the above tables, each secure device is a member of a number of sets A-E such that any two or more secure devices which are a member of a subset, are not a member of the same subset in another set. In this manner each secure device 4 will receive a unique combination of subset keys.

The keys are distributed among the secure devices 4 when the secure devices are initialized. As shown in fig. 2, each secure device 4 comprises a processor 5 and a memory 6, wherein the unique combination of subset keys is stored in the memory 6.

The control word used by the provider system 1 to scramble the content is encrypted in this example using the keys of the first set A, i.e. the keys A,a, A,b ... A,e. This requires five encrypted control messages to be added to the content for distribution together with the content. A header with an identifier identifying the key used to encrypt the control message is added to the control message.

When the scrambled content is received by the system 3, descrambling of the content occurs as follows. When

the secure device 4 is connected to the descrambling system 3, the processor 5 of the secure device 4 will forward the identifier of the first of its keys to a processor 7 of the descrambling system 3. The processor 7 receives the scrambled content together with the encrypted control messages and will send the control message with a corresponding identifier to the secure device 4 and the processor 5 will decrypt the encrypted control message using the corresponding key from the memory 6. The decrypted control word will be forwarded to the processor 7 for descrambling the content and in this manner the clear content is obtained.

If we assume that secure device #01 has been breached, the keys of the combination of keys stored in the memory 6 of this secure device should not be used anymore. This means that secure devices #02-#05 need to be provided with encrypted control messages encrypted by using keys B,b, B,c, B,d and B,e, for example. In this manner it is obtained that the information on the keys stored on secure device #01 is useless for the future.

It is noted that in the example given, after breaching three secure devices, there may be legal secure devices, the keys of which would be exposed. These secure devices can still be provided with an encrypted control message by using a key that is unique to the corresponding secure device. In this respect it is noted that each secure device of the complete set of secure devices will generally be provided with a unique key for forwarding messages to each secure device, if necessary. Further it is noted that the number of encrypted control messages increases each time that the system is breached. Of course, the example given is just for illustration purposes. Generally a set of secure devices will include a much larger number of secure devices which are divided into more sets and subsets than in the example described.

Further it is noted that further subdivisions into subsets, sub-subsets etc. can be made. Further, it is possible to divide the secure devices into entirely independent super sets, wherein keys are distributed within a super set

according to the method described.

In case wherein there is a regular online connection with the provider system, it is possible that the provider system 1 forwards a revocation message to all systems 3. This revocation message informs the systems 3 of the fact that the keys of a secure device of which the security has been breached, will not be used anymore. By means of this information, the remaining legal secure devices 4 which are a member of the same subset, will use another key of their own unique combination of keys in future and will provide the corresponding identifier to the descrambling system 3. In this manner the descrambling system will forward the correct encrypted control message to its secure device 4.

The invention can be advantageously used in any security system comprising a plurality of terminals and a plurality of secure devices, in particular in off-line applications. In case of terminals verifying a secure device by challenging the secure device to perform a cryptographic operation, for example in a zero knowledge protocol, the system operates as follows. A secret to be used in the zero knowledge protocol is encrypted using a key of the number of keys available in the system. The keys are distributed among the secure devices as described above. The encrypted secret is forwarded to the secure device with an identifier indicating the key to be used. If this key is available to the secure device, the secure device can decrypt the secret and can use this secret in the zero knowledge protocol. If a secure device is breached, the keys available to the breached device will not be used anymore and those legal secure device having the same keys as the breached device can communicate with the terminals by using another key of the keys available to these legal secure devices.

The invention is not restricted to the above described embodiments which can be varied within a number of ways within the scope of the claims.

CLAIMS

1. Method for distributing keys among a number of secure devices, wherein the secure devices are divided into sets (A,B,C,D,E), each set having a plurality of subsets (a,b,c,d,e), each subset comprising two or more secure devices having the same key which is unique for this subset, wherein each secure device is a member of a number of sets (A,B,C,D,E) such that two or more secure devices which are a member of a subset, are not a member of the same subset in another set.

2. Method for communicating with a number of secure devices, comprising providing a number of unique keys, said number of keys being divided into subsets (A,a;A,b;...E,d;E,e), providing a plurality of encrypted messages by encrypting at least one clear message using different keys of said number of keys, adding an identifier to each encrypted message identifying the key used, wherein only a plurality of the available number of keys are used to provide said encrypted messages, forwarding the encrypted messages to the secure devices, and decrypting the encrypted message in the secure device to obtain the clear message.

3. Method according to claim 2, used in a zero knowledge protocol, wherein the clear message is used by the secure device at least as part of a secret used in the zero knowledge protocol.

4. Method according to claim 2 used for scrambling a content for distribution among a number of users, comprising scrambling the content using a control word, wherein the control word is said clear message, wherein the scrambled content and the number of encrypted control messages are forwarded to all users.

5. Method according to claim 4, wherein a revocation message is forwarded to all users, said message identifying a plurality of keys which are revoked from said number of keys.

6. Method for descrambling a scrambled content, comprising receiving the scrambled content and receiving a

plurality of encrypted control messages, each encrypted control message having an identifier and containing a control word encrypted using a different key identified by the corresponding identifier, retrieving a first key identifier from a secure device having a plurality of keys with key identifiers, searching for an encrypted control message having an identifier corresponding to the retrieved identifier and decrypting in the secure device the encrypted control message found to obtain the control word, and descrambling the scrambled content by using the control word.

7. Method according to claim 6, wherein a next key identifier is retrieved from the secure device if an encrypted control message with the first retrieved key identifier can not be found.

8. Security system, comprising a plurality of terminals and a plurality of secure devices, each secure device comprising a processor and a memory for storing keys, wherein the secure devices are divided into sets (A,B,C,D,E), each set having a plurality of subsets (a,b,c,d,e), each subset being assigned a unique key from a number of unique keys (A,a;A,b;...E,d;E,e) and each subset comprising two or more of the secure devices, wherein the memory of each secure device contains a plurality of keys unique to different subsets such that the memory of each secure device contains a unique combination of unique subset keys, each terminal comprising means for forwarding an encrypted message to a secure device communicating with the terminal, wherein each encrypted message is obtained by encrypting at least one clear message using different keys of said number of keys, adding an identifier to each encrypted message identifying the key used, wherein only a plurality of the available number of keys are used to provide said encrypted messages, and decrypting the encrypted message in the secure device to obtain the clear message for further use.

9. Set of secure devices, such as smart cards, each secure device comprising a processor and a memory for storing keys, wherein the secure devices are divided into

sets (A,B,C,D,E), each set having a plurality of subsets (a,b,c,d,e), each subset being assigned a unique key and each subset comprising two or more of the secure devices, wherein the memory of each secure device contains a plurality of keys unique to different subsets such that the memory of each secure device contains a unique combination of unique subset keys.

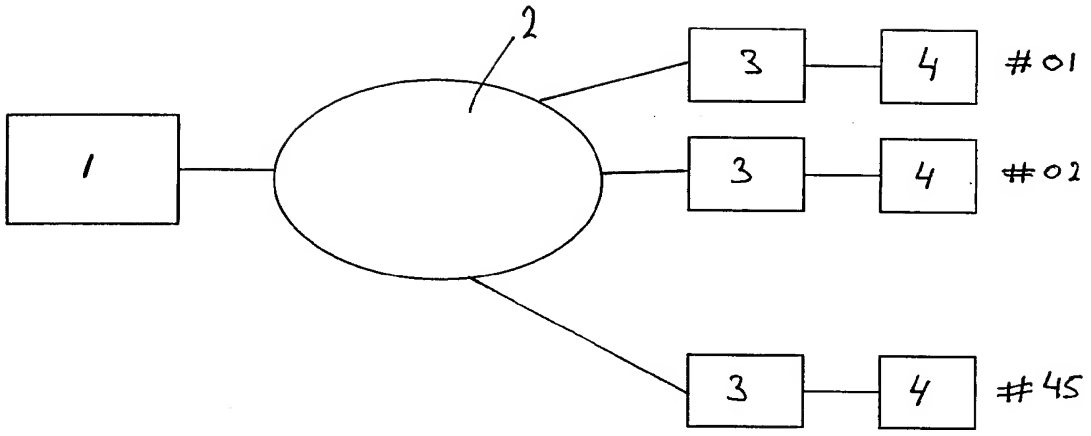


fig. 1

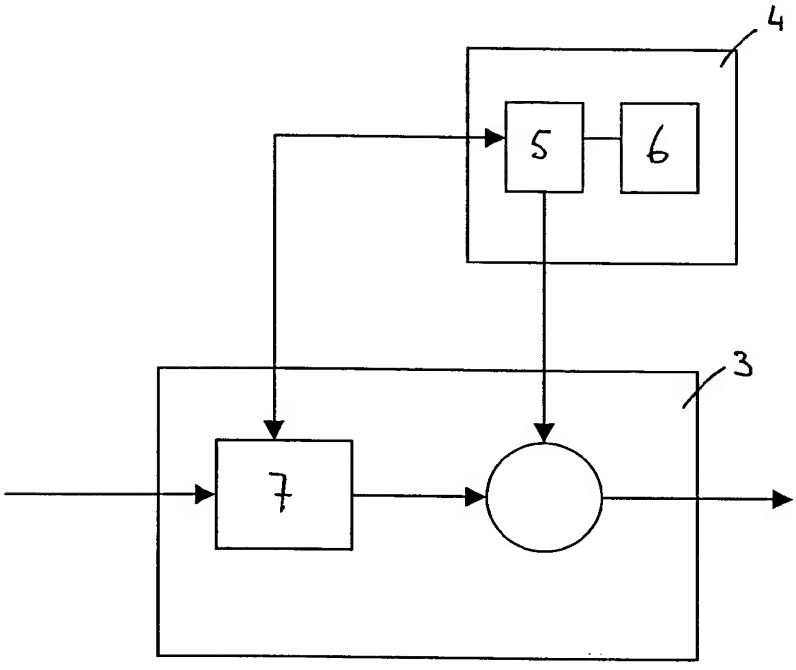


fig. 2

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/EP 00/09866

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BLUNDO C ET AL: "Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO '96, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 387-400, XP000626596 1996, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-61512-1 page 389 --- -/--	1-9

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 December 2000	05/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern: ıal Application No
PCT/EP 00/09866

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 641 103 A (ALGORITHMIC RES LTD) 1 March 1995 (1995-03-01) page 3, line 10 -page 17, line 1 ---	2-8
A	NAKAMURA H ET AL: "Hierarchical group oriented key management method HGK" PROCEEDINGS OF THE SIXTH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (CAT. NO.90TH0351-7), TUCSON, AZ, USA, 3-7 DEC. 1990, pages 44-49, XP002130707 1990, Los Alamitos, CA, USA, IEEE Comput. Soc. Press, USA ISBN: 0-8186-2105-2 page 2 -page 3 ---	2-8
A	SHIUH-JENG WANG ET AL: "A hierarchical and dynamic group-oriented cryptographic scheme" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, JAN. 1996, INST. ELECTRON. INF. & COMMUN. ENG, JAPAN, vol. E79-A, no. 1, pages 76-85, XP000558722 ISSN: 0916-8508 page 78, column 2 -page 79, column 1; figure 2 -----	2-8

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/EP 00/09866

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0641103 A	01-03-1995	IL 106796 A	20-11-1997
		US 5592552 A	07-01-1997